セキュリティ

ユーザー ガイド

First Edition: March 2006

製品番号： 406809-291

目次

1 セキュリティ機能

注記 セキュリティ ソリューションは、抑止効果を発揮することを目的として設計されています。製品の誤った取り扱いや盗難は、これらの抑止効果では防止できない場合があります。

注記 お使いのコンピュータでは、オンライン セキュリティ用の追跡および回復サービスである CompuTrace がサポートされています。コンピュータが盗まれた場合、権限のないユーザーがそのコンピュータからインターネットにアクセスしたかどうかを CompuTrace によって追跡できます。CompuTrace を使用するには、ソフトウェアを購入し、サービスに加入する必要があります。CompuTrace ソフトウェアの購入については、http://www.hpshopping.com にアクセスしてください。

お使いのコンピュータが備えているセキュリティ機能によって、コンピュータ自体、個人情報、およびデータをさまざまなリスクから保護できます。使用する必要があるセキュリティ機能は、コンピュータをどのように使用するかによって決まります。

Microsoft® Windows® オペレーティング システムも、一定のセキュリティ機能を提供しています。追加できるセキュリティ機能を以下の表に示します。これらの追加機能の大半は、Computer Setup ユーティリティ (以後 Computer Setup) で設定できます。

防御対象	使用するセキュリティ機能
コンピュータの不正使用	● パスワードまたはスマート カードの使用による電源投入時の認証 ● ProtectTools セキュリティ マネージャ
Computer Setup (F10) への不正アクセス	Computer Setup* のセットアップ パスワード
ハード ドライブのデータへの不正アクセス	Computer Setup* の DriveLock パスワード
Computer Setup (F10) の各種パスワードの不正リセット	Computer Setup の厳重セキュリティ機能
オプティカル ドライブ、フロッピー ディスク ドライブ、または内蔵ネットワーク アダプタからの不正な起動	Computer Setup* のブート オプション機能
Windows ユーザー アカウントへの不正アクセス	Credential Manager for ProtectTools
データへの不正アクセス	● ファイアウォール ソフトウェア ● Windows Updates ● ProtectTools セキュリティ マネージャ
Computer Setup の各種設定とその他のシステム識別情報への不正アクセス	Computer Setup* のセットアップ パスワード

防御対象	使用するセキュリティ機能
コンピュータの盗難	セキュリティ ケーブル スロット (別売のセキュリティ ケーブルとともに使用します)

*Computer Setup は、コンピュータの電源投入時または再起動時に F10 キーを押してアクセスするユーティリティであり、Windows ユーティリティではありません。Computer Setup を使用するとき、項目間を移動したり項目を選択したりするには、キーボード上のキーを使用する必要があります。

2 パスワード

ほとんどのセキュリティ機能では、パスワードが使用されます。パスワードを設定したときは、そのパスワードを常に書き留めておき、コンピュータから離れた安全な場所に保管してください パスワードに関する以下の考慮事項に注意してください。

- セットアップ パスワード、電源投入時パスワード、および DriveLock パスワードは、Computer Setup で設定し、システムの BIOS によって管理されます。
- Computer Setup で、ProtectTools セキュリティ マネージャのパスワードであるスマート カード PIN と内蔵セキュリティ パスワードを有効にすることで、ProtectTools の通常機能に加え、BIOS パスワードを保護できます。スマート カード PIN はサポートされているスマート カード リーダーで使用され、内蔵セキュリティ パスワードは別売の内蔵セキュリティ チップで使用されます。
- Windows パスワードは、Windows オペレーティング システムにのみ設定されます。
- Computer Setup に設定したセットアップ パスワードを忘れた場合、このユーティリティにはアクセスできません。
- Computer Setup で厳重セキュリティ機能を有効にした後でセットアップ パスワードまたは電源投入時パスワードを忘れた場合、コンピュータはアクセス不能になり、使用できなくなります。追加情報については、Customer Care またはサービス パートナに問い合わせてください。
- Computer Setup に設定した電源投入時パスワードとセットアップ パスワードを忘れた場合、コンピュータの電源を入れることも、休止状態を解除することもできなくなります。追加情報については、Customer Care またはサービス パートナに問い合わせてください。
- Computer Setup に設定した DriveLock のユーザー パスワードとマスタ パスワードを両方とも忘れた場合、これらのパスワードによって保護されたハード ドライブは永久にロックされ、使用できなくなります。

よく使用される Computer Setup と Windows の各種パスワードとそれぞれの機能を以下の表に示します。

Computer Setup のパスワード	機能
セットアップ パスワード	Computer Setup へのアクセスを保護します。
電源投入時パスワード	コンピュータの電源投入時、再起動時、または休止状態からの復帰時に、コンピュータのデータへのアクセスを保護します。
DriveLock マスタ パスワード	DriveLock によって保護されている内蔵ハード ドライブへのアクセスを保護します。DriveLock 保護を解除するためにも使用します。
DriveLock ユーザー パスワード	DriveLock によって保護されている内蔵ハード ドライブへのアクセスを保護します。

Computer Setup のパスワード	機能
スマート カード PIN	スマート カードと Java™ Card のデータへのアクセスを保護します。スマート カードまたは Java Card と、スマート カード リーダーが使用されているときに、コンピュータへのアクセスを保護します。
内蔵セキュリティ パスワード	BIOS パスワードとして有効にすると、コンピュータの電源投入時、再起動時、または休止状態からの復帰時に、コンピュータのデータへのアクセスを保護します。 このパスワードを使用するには、このセキュリティ機能をサポートする別売の内蔵セキュリティ チップが必要です。

Windows のパスワード	機能
管理者パスワード*	Windows の管理者レベルのデータへのアクセスを保護します。
ユーザー パスワード	Windows ユーザー アカウントへのアクセスを保護します。コンピュータのデータへのアクセスも保護します。スタンバイから再開するとき、または休止状態から復帰するときに入力する必要があります。
*Windows 管理者パスワードまたは Windows ユーザー パスワードの設定については、**[スタート > ヘルプとサポート]**を選択して、詳細を参照してください。	

パスワード設定時のガイドライン

Computer Setup 機能と Windows セキュリティ機能の両方で同じパスワードを使用できます。複数の Computer Setup 機能で同じパスワードを使用できます。

Computer Setup に設定されるパスワード

- Computer Setup に設定するパスワードは、任意の英数字を 32 文字まで組み合わせて指定できます。大文字と小文字の区別はありません。
- 設定時と入力時に同じキーを使用する必要があります。たとえば、キーボード上の数字キーを使用してパスワードを設定した場合は、内蔵テンキー上のキーを使用して入力すると、パスワードとして認識されません。

  注記　一部のモデルのテンキーは、キーボード上の数字キーとまったく同じように機能します。

- Computer Setup プロンプトで入力する必要があります。Windows に設定されるパスワードは、Windows プロンプトで入力する必要があります。

パスワードの作成および保存時のヒント

- パスワードを作成するときは、プログラムの要件に従う
- パスワードを書き留めておき、コンピュータから離れた安全な場所に保管する
- パスワードをコンピュータ上のファイルに保存しない
- 部外者が簡単に知ることができる名前などの個人情報を使用しない

Computer Setup のセットアップ パスワード

Computer Setup のセットアップ パスワードは、Computer Setup 内の各種設定とシステム識別情報を保護します。このパスワードを設定した場合は、Computer Setup にアクセスして変更を行うときにパスワードを入力する必要があります。

セットアップ パスワードの特徴

- Windows 管理者パスワードで代替できませんが、両方が同一であってもかまいません。
- 設定、入力、変更、または削除時に画面に表示されません。
- 設定時と入力時に同じキーを使用する必要があります。たとえば、セットアップ パスワードをキーボード上の数字キーを使用して設定した場合、内蔵テンキー上の数字キーを使用して入力すると、パスワードとして認識されません。
- 最長 32 文字まで英数字を組み合わせて指定できます。大文字と小文字の区別はありません。

セットアップ パスワードの設定

セットアップ パスワードの設定、変更、および削除は、Computer Setup で実行します。

このパスワードを管理するには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> Setup password]** (セットアップ パスワード) の順に選択し、Enter キーを押します。
   - セットアップ パスワードを設定するには、次の手順を行います。

     [New password] (新しいパスワード) フィールドと **[Verify new password]** (新しいパスワードの確認) フィールドにパスワードを入力し、F10 キーを押します。
   - 管理者パスワードを変更するには、次の手順を行います。

     [Old password] (古いパスワード) フィールドに現在のパスワードを、**[New password]** (新しいパスワード) フィールドと **[Verify new password]** (新しいパスワードの確認) フィールドに新しいパスワードを入力し、F10 キーを押します。
   - セットアップ パスワードを削除するには、次の手順を行います。

     [Old password] (古いパスワード) フィールドに現在のパスワードを入力し、F10 キーを押します。
3. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

セットアップ パスワードの入力

[Setup password] (セットアップ パスワード) プロンプトで、セットアップ パスワードを入力し (パスワードの設定時に使用したキーを使用します)、Enter キーを押します。正しいセットアップ パスワードを 3 回以内に入力できなかった場合、コンピュータを再起動してやり直す必要があります。

Computer Setup の電源投入時パスワード

Computer Setup の電源投入時パスワードは、コンピュータの不正使用を防止します。このパスワードを設定した場合は、コンピュータの電源を入れたときに毎回パスワードを入力する必要があります。

電源投入時パスワードの特徴

- 設定、入力、変更、または削除時に画面に表示されません。
- 設定時と入力時に同じキーを使用する必要があります。たとえば、電源投入時パスワードをキーボード上の数字キーを使用して設定した場合、内蔵テンキー上の数字キーを使用して入力すると、パスワードとして認識されません。
- 最長 32 文字まで英数字を組み合わせて指定できます。大文字と小文字の区別はありません。

電源投入時パスワードの設定

電源投入時パスワードの設定、変更、および削除は、Computer Setup で実行します。

このパスワードを管理するには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> Power-On password]** (電源投入時パスワード) を選択し、Enter キーを押します。
   - 電源投入時パスワードを設定するには、次の手順を行います。

     [New password] (新しいパスワード) フィールドと **[Verify new password]** (新しいパスワードの確認) フィールドにパスワードを入力し、F10 キーを押します。
   - 電源投入時パスワードを変更するには、次の手順を行います。

     [Old password] (古いパスワード) フィールドに現在のパスワードを、**[New password]** (新しいパスワード) フィールドと **[Verify new password]** (新しいパスワードの確認) フィールドに新しいパスワードを入力し、F10 キーを押します。
   - 電源投入時パスワードを削除するには、次の手順を行います。

     [Old password] (古いパスワード) フィールドに現在のパスワードを入力し、F10 キーを押します。
3. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

電源投入時パスワードの入力

[Power-on password] (電源投入時パスワード) プロンプトで、パスワードを入力し (パスワードの設定時に使用したキーを使用します)、Enter キーを押します。正しいパスワードを 3 回以内に入力できなかった場合、コンピュータの電源を切ってから再度電源を入れてやり直す必要があります。

再起動時の電源投入時パスワードの入力要求

電源投入時パスワードは、コンピュータの電源を入れたときだけでなく、コンピュータを再起動するたびに入力を要求するように設定できます。

Computer Setup でこの機能を有効または無効にするには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> Password options]** (パスワード オプション) **[> Require password on restart]** (再起動時にパスワードが必要) の順に選択し、Enter キーを押します。
3. 矢印キーを使用してこのパスワード機能を有効または無効にし、F10 キーを押します。
4. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

Computer Setup の DriveLock

注意　DriveLock によって保護されたハード ドライブが永久に使用不能になる事態を回避するために、DriveLock ユーザー パスワードと DriveLock マスタ パスワードをコンピュータとは別の安全な場所に記録しておいてください。両方の DriveLock パスワードを忘れた場合、ハード ドライブは永久にロックされ、使用できなくなります。

DriveLock は、ハード ドライブのデータへの不正アクセスを防止します。DriveLock は、コンピュータの内蔵ハード ドライブにのみ適用できます。ドライブに DriveLock 保護を適用した場合、ドライブにアクセスするにはパスワードを入力する必要があります。DriveLock パスワードを入力してドライブにアクセスするには、ドライブが別売のドッキング デバイスや外付けマルチベイではなくコンピュータに装着されている必要があります。

内蔵ハード ドライブに DriveLock 保護を適用するには、ユーザー パスワードとマスタ パスワードを Computer Setup に設定する必要があります。DriveLock 保護の使用に関する以下の考慮事項に注意してください。

- ハード ドライブに DriveLock 保護を適用した場合、ユーザー パスワードまたはマスタ パスワードを入力しないとハード ドライブにアクセスできません。
- ユーザー パスワードの所有者は、保護されるハード ドライブを日常的に使用するユーザーにします。マスタ パスワードの所有者は、システム管理者でもハード ドライブを日常的に使用するユーザーのどちらでもかまいません。
- ユーザー パスワードとマスタ パスワードは、同一でもかまいません。
- ユーザー パスワードまたはマスタ パスワードを削除するには、ドライブから DriveLock 保護を解除することが唯一の方法です。ドライブから DriveLock 保護を解除するには、必ずマスタ パスワードを使用する必要があります。

注記　電源投入時パスワードと DriveLock ユーザー パスワードが同一の場合は、両方のパスワードではなく、電源投入時パスワードのみの入力を求められます。

DriveLock パスワードの設定

Computer Setup の DriveLock 設定にアクセスするには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> DriveLock password]** (DriveLock パスワード) の順に選択し、Enter キーを押します。
3. 保護対象となるハード ドライブの場所を選択し、F10 キーを押します。
4. 矢印キーを使用して **[Protection]** (保護) フィールドの **[Enable]** (有効化) を選択し、F10 キーを押します。
5. 警告を読みます。続行するには、F10 キーを押します。
6. **[New password]** (新しいパスワード) フィールドと **[Verify new password]** (新しいパスワードの確認) フィールドにパスワードを入力し、F10 キーを押します。
7. **[New password]** (新しいパスワード) フィールドと **[Verify new password]** (新しいパスワードの確認) フィールドにマスタ パスワードを入力し、F10 キーを押します。
8. 選択済みのドライブに対する DriveLock 保護を確認するために、確認フィールドに「DriveLock」と入力し、F10 キーを押します。
9. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

DriveLock パスワードの入力

ハード ドライブが (別売のドッキング デバイスや外付けマルチベイではなく) コンピュータに装着されていることを確認してください。

[DriveLock HDD Bay Password] (DriveLock HDD ベイ パスワード) プロンプトで、ユーザー パスワードまたはマスタ パスワードを入力し (パスワードの設定時に使用したキーを使用します)、Enter キーを押します。

正しいパスワードを 2 回以内に入力できなかった場合、コンピュータを再起動してやり直す必要があります。

DriveLock パスワードの変更

Computer Setup の DriveLock 設定にアクセスするには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> DriveLock password]** (DriveLock パスワード) の順に選択し、Enter キーを押します。
3. 矢印キーを使用して内蔵ハード ドライブの場所を選択し、F10 キーを押します。
4. 矢印キーを使用して、変更するパスワードのフィールドを選択します。**[Old password]** (古いパスワード) フィールドに現在のパスワードを、**[New password]** (新しいパスワード) フィールドと **[Verify new password]** (新しいパスワードの確認) フィールドに新しいパスワードを入力します。F10 キーを押します。
5. **[Confirm New Password]** (新しいパスワードの確認) フィールドに新しいパスワードを再度入力し、Enter キーを押します。
6. 設定通知メッセージが表示されたら、Enter キーを押して変更を保存します。
7. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

DriveLock 保護の解除

Computer Setup の DriveLock 設定にアクセスするには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> DriveLock password]** (DriveLock パスワード) の順に選択し、Enter キーを押します。
3. 矢印キーを使用して内蔵ハード ドライブの場所を選択し、F10 キーを押します。
4. 矢印キーを使用して **[Protection]** (保護) フィールドの **[Disable]** (無効化) を選択し、F10 キーを押します。

5. **[Old password]** (古いパスワード) フィールドにマスタ パスワードを入力します。F10 キーを押します。

6. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

3 Computer Setup のセキュリティ機能

デバイスのセキュリティ

Computer Setup の [Boot options] (ブート オプション) メニューまたは [Port options] (ポート オプション) メニューから、システム デバイスを有効または無効にできます。

Computer Setup でシステム デバイスを無効にする、または再度有効にするには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[System Configuration]** (システム構成) **[> Boot options]** (ブート オプション) または **[System Configuration]** (システム構成) **[> Port options]** (ポート オプション) の順に選択し、設定を変更します。
3. 設定を確認するには、F10 キーを押します。
4. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

Computer Setup の厳重セキュリティ

注意 コンピュータが永久に使用不能になる事態を回避するために、設定されたセットアップ パスワード、電源投入時パスワード、またはスマート カード PIN をコンピュータとは別の安全な場所に記録しておいてください。これらのパスワードまたは PIN がなければ、コンピュータのロックを解除することはできません。

厳重セキュリティ機能は、システムへのアクセスを許可する前に、設定済みのセットアップ パスワード、電源投入時パスワード、またはスマート カード PIN を使用してユーザー認証を実行することにより、電源投入時のセキュリティを強化します。

厳重セキュリティの設定

Computer Setup で厳重セキュリティを有効にするには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> Password options]** (パスワード オプション) の順に選択し、Enter キーを押します。
3. 矢印キーを使用して、**[Stringent security]** (厳重セキュリティ) フィールドを選択します。
4. 警告を読みます。続行するには、F10 キーを押します。
5. コンピュータの電源を入れるたびにこの機能を有効にするには、F10 キーを押します。
6. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

厳重セキュリティの解除

Computer Setup で厳重セキュリティを解除するには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. 矢印キーを使用して **[Security]** (セキュリティ) **[> Password options]** (パスワード オプション) の順に選択し、Enter キーを押します。
3. 矢印キーを使用して **[Stringent security]** (厳重セキュリティ) フィールドの **[Disable]** (無効化) を選択し、F10 キーを押します。
4. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

Computer Setup のシステム情報

Computer Setup のシステム情報機能は、以下の 2 種類のシステム情報を提供します。

- コンピュータ モデルとバッテリ パックに関する識別情報
- プロセッサ、キャッシュ、メモリ、ROM、ビデオとキーボード コントローラのバージョンに関する仕様情報

この全般的なシステム情報を表示するには、矢印キーを使用して **[File]** (ファイル) **[> System Information]** (システム情報) を選択します。

注記　この情報への不正アクセスを防止するには、Computer Setup でセットアップ パスワードを作成する必要があります。追加情報については、「セットアップ パスワードの設定」を参照してください。

Computer Setup のシステム ID

Computer Setup のシステム ID 機能は、コンピュータ アセット タグとオーナーシップ タグの表示または入力を可能にします。

注記　この情報への不正アクセスを防止するには、Computer Setup でセットアップ パスワードを作成する必要があります。追加情報については、「セットアップ パスワードの設定」を参照してください。

この機能を管理するには、次の手順を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に [F10 = ROM Based Setup] (ROM ベースのセットアップ) というメッセージが表示されている間に F10 キーを押して、Computer Setup を起動します。
2. システム コンポーネントの識別タグ ID を表示または入力するには、矢印キーを使用して **[Security]** (セキュリティ) **[> System IDs]** (システム ID) の順に選択します。
3. 情報または設定を確認するには、F10 キーを押します。
4. 設定を保存するには、矢印キーを使用して **[File]** (ファイル) **[> Save changes and exit]** (設定を保存して終了) の順に選択してから、画面の説明に沿って操作します。

   設定は、コンピュータを再起動したときに有効になります。

4 ウイルス対策ソフトウェア

コンピュータを使用して電子メール、ネットワーク、またはインターネット アクセスを行うと、コンピュータ ウイルスに感染することがあります。コンピュータ ウイルスは、オペレーティング システム、アプリケーション、またはユーティリティを無効にしたり、異常な動作を起こさせたりすることができます。

ウイルス対策ソフトウェアは、ウイルスの大半を検出して破棄することができ、ほとんどの場合、ウイルスを原因とする損傷を修復できます。新たに発見されるウイルスに対して継続的に防護するには、ウイルス対策ソフトウェアを更新する必要があります。

このコンピュータには、Norton Internet Security がプリインストールされています。Norton Internet Security ソフトウェアの使用方法については、**[スタート > すべてのプログラム > Norton Internet Security > ヘルプとサポート]** の順に選択してください。

コンピュータ ウイルスについて詳しくは、[ヘルプとサポート センター] の [検索] フィールドに「ウイルス対策」と入力してください。

5 ファイアウォール ソフトウェア

コンピュータを使用して電子メール、ネットワーク、またはインターネット アクセスを行うと、権限のない人間によって、個人情報やコンピュータに関する情報にアクセスされてしまうことがあります。コンピュータにプリインストールされているファイアウォール ソフトウェアを使用して、プライバシーを保護してください。

ファイアウォール機能には、着信および発信トラフィックをモニタするためのロギング、レポーティング、および自動アラームが含まれます。詳しくは、ファイアウォールのマニュアルを参照するか、ファイアウォールの製造元に問い合わせてください。

注記　特定の状況下では、ファイアウォールがインターネット ゲームへのアクセスをブロックしたり、ネットワーク上のプリンタやファイルの共有に干渉したり、許可されている電子メールの添付ファイルをブロックしたりすることがあります。問題を一時的に解決するには、ファイアウォールを無効にして目的のタスクを実行した後で、ファイアウォールを再度有効にします。問題を永久に解決するには、ファイアウォールを再設定します。

6　クリティカル セキュリティ アップデート (一部のモデルのみ)

△ **注意**　セキュリティ違反やコンピュータ ウイルスからコンピュータを保護するには、アラートを受信したらすぐに Microsoft からオンライン クリティカル アップデートをインストールします。

コンピュータの設定後に提供された追加アップデートを反映するために、*Critical Security Updates for Windows XP* ディスクがコンピュータに添付されていることがあります。

Critical Security Updates for Windows XP ディスクを使用してシステムを更新するには、次の手順を行います。

1. ディスクをドライブに挿入します (インストール アプリケーションが自動的に実行されます)。
2. 画面の説明に沿って操作し、すべてのアップデートをインストールします (これは、数分かかることがあります)。
3. ディスクを取り出します。

コンピュータが出荷された後で、オペレーティング システムやその他のソフトウェアに対する追加アップデートが使用可能になることがあります。すべての使用可能なアップデートが常にコンピュータにインストールされているようにするには、次のことを行います。

- Windows Update を毎月実行して、Microsoft から最新のソフトウェアをインストールします。
- アップデートがリリースされたとき、Microsoft の Web サイトまたはヘルプとサポート センターの更新リンクからアップデートを取得します。

7 ProtectTools セキュリティ マネージャ (一部のモデルのみ)

一部のモデルには、ProtectTools セキュリティ マネージャがプリインストールされています。このソフトウェアには、Microsoft Windows コントロール パネルからアクセスできます。このソフトウェアは、コンピュータ、ネットワーク、重要データへの不正アクセスを防止するために役立つセキュリティ機能を提供します。ProtectTools セキュリティ マネージャは、以下のモジュールの追加による機能強化を提供するセキュリティ コンソールです。

- Embedded Security for ProtectTools
- Credential Manager for ProtectTools
- BIOS Configuration for ProtectTools
- Smart Card Security for ProtectTools
- Java Card Security for ProtectTools

コンピュータ モデルによって、アドオン モジュールは、プリインストールされているか、プリロードされているか、HP の Web サイトからダウンロードできます。詳しくは、http://www.hp.com にアクセスしてください。

Embedded Security for ProtectTools

注記 Embedded Security for ProtectTools を使用するには、別売のトラステッド プラットフォーム モジュール (TPM) 内蔵セキュリティ チップがコンピュータにインストールされている必要があります。

Embedded Security for ProtectTools には、ユーザー データや証明書に対する不正アクセスを防止する以下のセキュリティ機能があります。

- オーナーシップやオーナー パスワードの管理などの管理機能
- ユーザー登録やユーザー パスワードの管理などのユーザー機能
- ユーザー データを保護するための拡張 Microsoft EFS や Personal Secure Drive の設定を含む設定構成
- キー階層のバックアップや復元などの管理機能
- 内蔵セキュリティ使用時にデジタル証明書の保護操作を行うためのサードパーティ アプリケーション (Microsoft Outlook や Internet Explorer など) のサポート

別売の TPM 内蔵セキュリティ チップは、ProtectTools セキュリティ マネージャ ツールの他の機能を拡張かつ有効にします。たとえば、Credential Manager for ProtectTools は、ユーザーが Windows にログインしたときに、認証要素として内蔵チップを使用できます。一部のモデルでは、TPM 内蔵セキュリティ チップは、BIOS Configuration for ProtectTools からアクセスされる拡張 BIOS セキュリティ機能も有効にします。

詳しくは、Embedded Security for ProtectTools のヘルプを参照してください。

Credential Manager for ProtectTools

Credential Manager for ProtectTools には、コンピュータに対する不正アクセスを防止する以下のセキュリティ機能があります。

- Microsoft Windows にログインするときにパスワードの代わりにスマート カードなどを使用してログインする機能
- Web サイト、アプリケーション、および保護されたネットワーク リソースの証明書を自動的に記憶するシングル サインオン機能
- スマート カードや指紋リーダーなどの別売のセキュリティ デバイスのサポート

詳しくは、Credential Manager for ProtectTools のヘルプを参照してください。

BIOS Configuration for ProtectTools

BIOS Configuration for ProtectTools は、BIOS (Computer Setup) セキュリティと ProtectTools セキュリティ アプリケーション内の設定へのアクセスを提供します。これにより、ユーザーは、Computer Setup によって管理されているシステム セキュリティ機能に簡単にアクセスできます。

BIOS Configuration for ProtectTools を使用して、以下の操作を実行できます。

- 電源投入時パスワードとセットアップ パスワードの管理
- スマート カード パスワードや内蔵セキュリティ認証の有効化などのその他の電源投入時認証機能の設定
- CD-ROM ブートや複数のハードウェア ポートなどのハードウェア機能の有効化と無効化
- MultiBoot の有効化やブート順序の変更などを含むブート オプションの設定

注記　BIOS Configuration for ProtectTools の機能の大半は、Computer Setup でも使用できます。

詳しくは、BIOS Configuration for ProtectTools のヘルプを参照してください。

Smart Card Security for ProtectTools

Smart Card Security for ProtectTools は、スマート カードの設定と、別売のスマート カード リーダーを装着したコンピュータの設定を管理します。

注記　スマート カードと Java Card は、どちらもスマート カード リーダーを使用します。

Smart Card Security for ProtectTools を使用して、以下の操作を実行できます。

- スマート カード セキュリティ機能へのアクセス。セキュリティの強化は、別売の ProtectTools スマート カードとスマート カード リーダーによってサポートされます。
- ProtectTools スマートカードを初期化して、Credential Manager for ProtectTools で使用できるようにする
- BIOS を操作して、プリブート環境でのスマート カード認証を可能にし、管理者とユーザーに対して別々のスマート カードを設定する。これにより、ユーザーがオペレーティング システムをロードするには、スマート カードを挿入し、オプションで PIN を入力する必要があります。
- スマート カードのユーザーを認証するために使用されるパスワードの設定と変更
- スマート カード上に保存されるスマート カード BIOS パスワードのバックアップと復元

詳しくは、Smart Card Security for ProtectTools のヘルプを参照してください。

Java Card Security for ProtectTools

Java™ Card Security for ProtectTools は、別売のスマート カード リーダーを備えたコンピュータでの Java Card のセットアップと設定を管理します。

注記 Java Card とスマート カードは、どちらもスマート カード リーダーを使用します。

Java Card Security for ProtectTools を使用して、以下の操作を実行できます。

- Java Card セキュリティ機能へのアクセス。セキュリティの強化は、別売の ProtectTools Java Card とスマート カード リーダーによってサポートされます。
- Credential Manager for ProtectTools で Java Card を使用するための一意な PIN の作成
- BIOS を操作して、ブート前の環境での Java Card 認証を有効にし、管理者とユーザーに対して別々の Java Card を設定する。これにより、ユーザーがオペレーティング システムをロードするには、Java Card を挿入し、PIN を入力する必要があります。
- Java Card ユーザーの認証に使用される ID の設定と変更
- Java Card に保存される Java Card ID のバックアップと復元

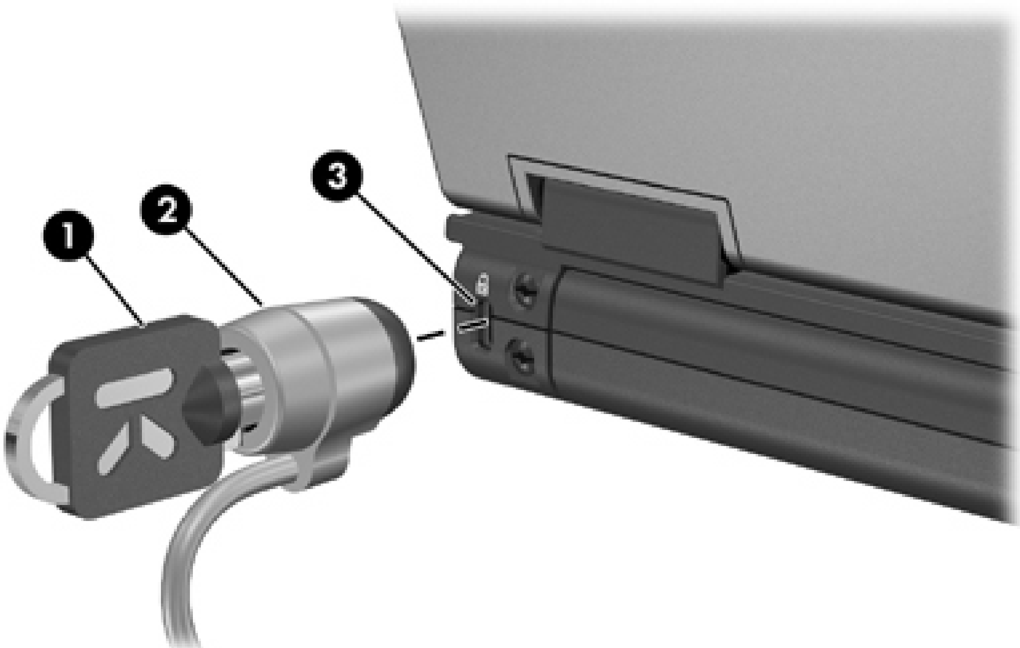
詳しくは、Java Card Security for ProtectTools のヘルプを参照してください。

8　セキュリティ ケーブル

注記　セキュリティ ケーブルは、抑止効果を発揮することを目的としていますが、コンピュータの誤った取り扱いや盗難を防止できるとは限りません。

セキュリティ ケーブルを取り付けるには、次の手順を行います。

1. セキュリティ ケーブルを固定された物体に巻きつけます。
2. キー **(1)** をケーブル ロック **(2)** に差し込みます。
3. ケーブル ロックをコンピュータのセキュリティ ケーブル スロット **(3)** に挿入し、キーを使用してケーブル ロックを固定します。

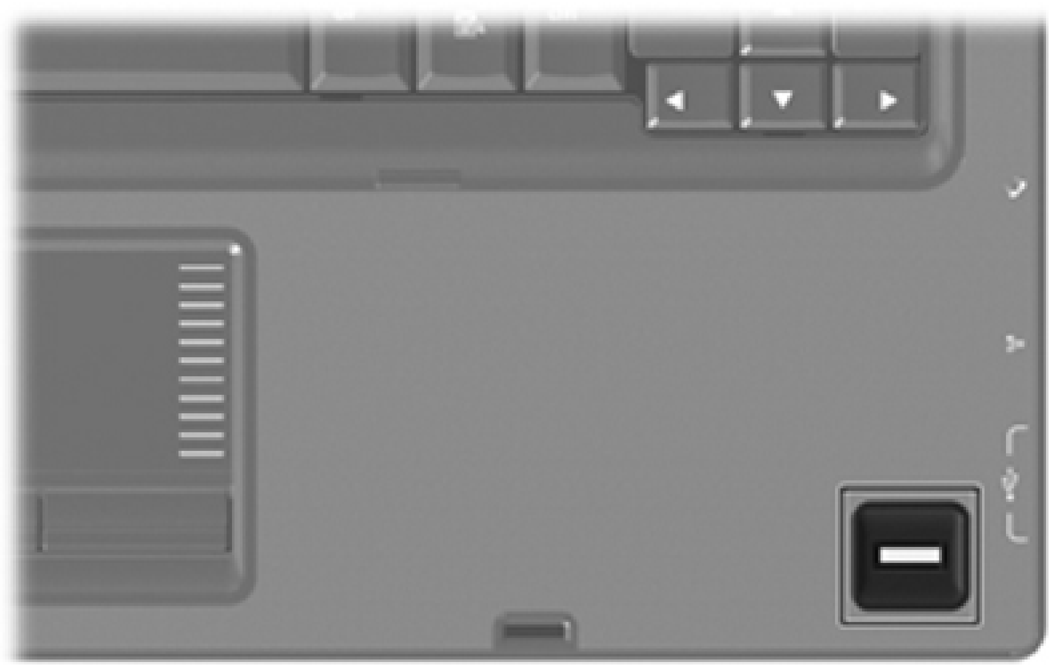


注記　実際のコンピュータは、図とは異なる場合があります セキュリティ ケーブル スロットの位置は、モデルによって異なります。

9　指紋リーダー (一部のモデルのみ)

指紋リーダーの使用

注記　指紋リーダーの位置は、モデルによって異なります。



指紋の登録

指紋リーダーを使用すると、Windows パスワードの代わりに ProtectTools セキュリティ マネージャに登録された指紋を使用して Windows にログオンできます。

指紋リーダーが HP コンピュータに内蔵されている場合でも、オプションとして外付けされている場合でも、指紋を使用して Windows にログインするには、以下の 2 つの手順に従う必要があります。

1. 指紋リーダーを設定します。
2. 登録された指紋を使用して、Windows にログオンします。

手順 1: 指紋リーダーの設定

注記　別売の指紋リーダーを使用する場合は、以下の手順を実行する前に、コンピュータにリーダーを接続してください。

指紋リーダーをセットアップするには、次の手順を行います。

1. Windows で、タスクバーの通知領域にある **[Credential Manager]** アイコンをダブルクリックします。

   - または -

   [スタート > すべてのプログラム > ProtectTools Security Manager] の順に選択し、左側の **[Credential Manager]** タブをクリックします。

2. [My Identity] ページで、ページの右下隅にある **[Log On]** (ログオン) をクリックします。

   Credential Manager ログオン ウィザードが開きます。

3. [Introduce Yourself] (自己紹介) ページで、[Next] (次へ) をクリックしてデフォルトのユーザー名をそのまま使用します。

   注記　このコンピュータに他のユーザーが登録されている場合は、Windows ユーザー名を入力することで、指紋を登録する必要がある人物を選択できます。

4. [Enter Password] (パスワードの入力) ページで、ユーザーの Windows パスワードを入力します (設定されている場合)。それ以外の場合は、**[Finish]** (終了) をクリックします。

5. [My Services and Applications] ページで、**[Register Fingerprints]** (指紋の登録) をクリックします。

   注記　デフォルトでは、少なくとも 2 本の指の指紋を登録する必要があります。

6. Credential Manager 登録ウィザードが開いているときに、指紋センサーの上に、指をゆっくりと押し付けます。

   注記　右手の人差し指が、第 1 指紋を登録するためのデフォルトの指です。このデフォルトは、最初に登録する指をクリックするか、左手または右手をクリックすることで変更できます。指をクリックすると、その指が選択されたことを示すために、輪郭が強調表示されます。

7. 画面上の指が緑色に変わるまで、同じ指を指紋センサーの上に置いたままにします。

   注記　1 回の読み取りが終わるたびに進捗インジケータが先に進みます。指紋を登録するには、複数回の読み取りが必要です。

   注記　指紋登録処理中に始めからやり直す必要がある場合は、画面上の強調表示されている指を右クリックし、**[Start Over]** (やり直し) をクリックします。

8. 次に登録する別の指を画面上でクリックし、手順 6 と 7 を繰り返します。

   注意　設定を完了するには、少なくとも 2 本の指を登録する必要があります。

注記　少なくとも 2 本の指を登録する前に **[Finish]** (終了) をクリックすると、エラー メッセージが表示されます。続行するには、**[OK]** をクリックします。

9. 少なくとも 2 本の指を登録した後、**[Finish]** (終了) をクリックし、**[OK]** をクリックします。
10. 別の Windows ユーザーのために指紋リーダーを設定するには、そのユーザーとして Windows にログオンし、手順 1 ～ 9 を繰り返します。

手順 2: 登録された指紋を使用した Windows へのログオン

登録された指紋を使用した Windows へのログオン

1. 指紋登録の直後に、Windows を再起動します。
2. 画面の左上隅にある **[Log on to Credential Manager]** (Credential Manager にログオン) をクリックします。
3. **[Credential Manager Logon Wizard]** ダイアログ ボックスで、ユーザー名をクリックする代わりに、登録済みのいずれかの指を使用して Windows にログオンします。
4. Windows パスワードを入力して、指紋とパスワードを関連付けます。

注記　指紋を使用して初めて Windows にログオンしたとき、Windows パスワードが設定されている場合は、Windows パスワードと指紋を関連付けるためにパスワードを入力する必要があります。パスワードと指紋が関連付けられた後は、指紋リーダーを使用するときに再度パスワードを入力する必要はありません。

索引